UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation	Case Nos. 13-MAG-2814; M9-150

REPLY IN SUPPORT OF MICROSOFT'S OBJECTIONS TO THE MAGISTRATE'S ORDER DENYING MICROSOFT'S MOTION TO VACATE IN PART A SEARCH WARRANT SEEKING CUSTOMER INFORMATION LOCATED OUTSIDE THE UNITED STATES

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Federal Statutes

Rules

Other Authorities

I. Introduction and Summary of Argument

The Government builds its entire argument on the quicksand foundation of a single flawed premise: that a customer's electronic letters and personal documents are Microsoft's own business records. Thus, it contends, those private communications are subject to the rule that companies under subpoena must "disclose" *their own* business records, wherever in the world they may be. But private emails stored in a password-protected digital lockbox are the property of the customer, not Microsoft's discoverable business records. A customer's email account is an electronic "cache of sensitive personal information" that is saturated with the highest constitutional privacy rights. *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). Whether an FBI agent personally captures the data or the Government conscripts an email provider to do it, such an intrusion upon privacy is the definition of a search and seizure. Just as a subpoena could compel a bank to disclose its ledger of transactions, but not the contents of a customer's safe deposit box, a subpoena could require Microsoft to produce its records *about* a customer's account, but not a customer's private email content. The Government can reach that content only through a warranted search and seizure.

Here, that search and seizure would occur in Ireland. This Warrant is invalid because Congress has not expressed any intention (much less a clear one) to allow the Government to require a provider to conduct searches and seizures of their customers' private communications in foreign lands. This is a textbook case of why the Supreme Court has repeatedly embraced a presumption against extraterritoriality. If this Court rules that the U.S. Government may unilaterally reach into foreign countries and expose their citizens' personal digital letters, the United States and its citizens cannot complain when foreign governments do the same to email content stored here. That is why the Government is wrong to say (at 25) that "[n]o valid privacy interest is vindicated" by Microsoft's position. The American people will think their constitutionally recog-

nized rights are very much at stake when a foreign government invokes this "business records" precedent to order technology companies to access U.S. servers and "disclose" all of the private correspondence of a New York Times reporter, a Member of Congress, or a federal judge.

II. Argument

A. The Government's Extraterritoriality Analysis Turns On The Flawed Premise That An Account Owner's Private Email Contents Are Microsoft's Own "Business Records."

Microsoft's opening brief explains that 18 U.S.C. § 2703(a) does not authorize the Government to conscript Microsoft to search for and seize a customer's email content stored abroad. The Government does not dispute the core legal premises of this argument:

1. The Electronic Communications Privacy Act ("ECPA") does not expressly authorize courts to issue warrants for extraterritorial searches and seizures of email content. *See* Opening Br. ("OB") 17-18.

2. "When a statute gives no clear indication of an extraterritorial application, it has none." *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010); OB 19-21.

3. The Government cannot conscript a private party to do what it cannot lawfully do itself. OB 21 (citing *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614 (1989)).

Rather, the Government simply disputes that any search and seizure takes place at all when the Government orders Microsoft to search for and seize a customer's email content, regardless of whether that content is located abroad or in the United States. The Government says warrants served under § 2703(a) require only that a provider produce "its own records," and thus are "functionally similar to subpoenas." U.S. Br. 8, 14. It contends that, under U.S. and international law, court orders asking a company to "disclose" its own business records, wherever in the world they may be, are routine, making the consent, notice, and/or cooperation of another country unnecessary. U.S. Br. 3, 12-13, 20-23 (citing *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) ("*BNS*"), and Restatement (Third) of the Foreign Relations Law of the United States ("Restatement") § 442). This interpretation of ECPA is the only

way the Government can conclude there is no impermissible extraterritorial application of the statute here. The Government's argument thus rises or falls on the premise that the email content at issue constitutes Microsoft's records subject to the *BNS* doctrine. The point is so central to the Government's position that it describes customers' personal email content as Microsoft's own business "records" no fewer than 60 times, starting on the cover of its brief.

The premise is dead wrong—so obviously wrong that the Government avoids mentioning the two cases that disprove it. The first is *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), which observed that stored email content contains individuals' "sensitive and intimate information," and worried that "government agents" who access that content have "the ability to peer deeply into [the owner's] activities." *Id.* at 284. More recently, in *Riley*, a unanimous Supreme Court affirmed that such electronic files contain "[t]he sum of an individual's private life," including "a record of all his communications," "a thousand photographs," and materials like "a prescription, a bank statement, a video." 134 S. Ct. at 2489. We entrust our highly sensitive email content to providers to keep it safe, not to read or use it themselves.[1] *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176-77 (9th Cir. 2010). Because customers have a reasonable "expectation of privacy" in email content, a "search occurs when the government" retrieves it without their authorization. *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

"The fact that the records [are] physically in the possession of" a caretaker is "of no consequence," absent "proof . . . that [the owner] had turned over his personal records to [the caretaker] to become part of its files and records." *United States v. Guterma*, 272 F.2d 344, 346 (2d Cir. 1959). Particularly when they are under the owner's lock and key (here by password), per-

[1] That a provider may "reserve[] the right to access [a customer's] emails for certain purposes," such as ensuring security, does not "extinguish [the customer's] reasonable expectation of privacy" in email content or cause it to become the provider's property. *Warshak*, 631 F.3d at 286-87.

sonal items remain in the "constructive possession" of the owner. *Id.* Accordingly, they cannot be seized "through the mere procedural device of compelling a third-party naked possessor to produce and deliver them." *Id.* at 346 (internal quotation marks omitted). Even if such a production order were issued by a neutral magistrate based on probable cause, it would still effect a search of an individual's private papers, not a request for the third-party custodian's records. Because a customer's emails are not Microsoft's "own records," U.S. Br. 14, the *BNS* line of cases, addressing disclosure of a company's own business records, has no application here.

The distinction is so fundamental that we take it for granted in the physical world. The government may compel Citibank by subpoena to divulge information about when a customer accessed a safe deposit box or made particular transactions, because those records are the *bank's* and contain information communicated to it "in the ordinary course of business." *United States v. Miller*, 425 U.S. 435, 442 (1976). But no subpoena (or anything "functionally similar" to a subpoena) could command Citibank to "disclose" the private letters kept in the customer's safe deposit box, even though they are, in some sense, in the bank's possession, custody or control. The Government may subpoena UPS to disclose its records of where a customer shipped packages, but any government-directed exploration of a package's contents would be a search because it would invade the reasonable expectation that sealed contents will remain private. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984). And while the Government may subpoena Marriott's guest registry, it cannot impound the diary from a guest's hotel room drawer except through a search and seizure.

Within the United States, seizing such private materials held by a custodian requires a search and seizure warrant. Beyond our borders, the Government cannot conscript the custodian's employees at a foreign branch to execute the search and seizure on the Government's behalf

because no statute expressly authorizes it to do so abroad. In the absence of that authority, to obtain the private content of a safe deposit box (or an envelope or a hotel room) located abroad, international law requires the Government to seek assistance from the government of the country where the evidence resides, through an MLAT or other forms of bilateral cooperation. *See, e.g.*, *Miller v. United States*, 955 F. Supp. 795, 796-97 (N.D. Ohio 1996) (Dutch authorities confiscated contents of safe deposit box at the request of U.S. authorities pursuant to a bilateral treaty).

Under *Warshak* and *Riley*, the same analysis that applies to physical correspondence sitting in a foreign safe deposit box or UPS envelope applies to digital correspondence in the lockbox of a foreign server. When a global law firm stores its privileged communications or a pharmaceutical company stores its trade secrets on Microsoft's servers, that information belongs to those customers; Microsoft has no right to casually peruse them, and they do not convert into Microsoft's own business records. The Government thus could not obtain them by serving a subpoena on Microsoft, regardless of where the content is kept. Whether domestically or abroad, the Government may procure customers' electronic content from a third-party provider only by executing a search and seizure—not by subpoena—just as it must to access a bank customer's safe deposit box, whether in New York or Dublin.[2] Indeed, if the Government were correct that a provider's compliance with a warrant like this one involved only gathering "its own records," then there would have been no seizure nor unconstitutional infringement of Steven Warshak's

[2] Microsoft thus does *not* take the anomalous position that the Government could obtain customers' email content stored abroad with a subpoena but not a warrant. *Contra* U.S. Br. 16. Rather, such content is *never* obtainable by subpoena issued to a third party like Microsoft, and *only ever* obtainable through a valid search and seizure, wherever it is. *See Warshak*, 631 F.3d at 286. For similar reasons, the Government's "upside-down pyramid" characterization of the statute (U.S. Br. 6) misses the point that no private content is obtainable by subpoena. That characterization is flawed in any event because it fails to account for the different notice requirements and degrees of judicial discretion that apply to subpoenas and warrants. *See* OB 12-13.

expectation of privacy at all. Yet *Warshak* held the opposite: The Government, via "his Internet Service Provider," violated the Fourth Amendment by engaging in an unwarranted "*ex parte* seizure of approximately 27,000 of his private emails." *Warshak*, 631 F.3d at 282. Having acquiesced in *Warshak*'s holding, the Government cannot now suggest retrieving a customer's emails involves anything other than a search and seizure of the customer's private "papers and effects."

The statutory text confirms Congress did not view the content of a customer's emails as the provider's own business records. Congress defined "records" as "not including the contents of communications." § 2703(c). The Government ignores this express distinction. But that distinction affects whether the Government may obtain the different types of information through a search and seizure, or merely a request for production. ECPA allows the Government to "require the disclosure . . . of [certain email contents] *only pursuant to a warrant*," which the Government may command the provider to execute on its behalf. § 2703(a) (emphasis added). In contrast, the Government may obtain "record[s] or other information" belonging to the provider by lesser forms of process directed to the provider itself, like a subpoena, § 2703(c), or an ECPA-specific "court order," § 2703(d). The legislative history supports this point. The House stated that electronic communications "contents are analogous to items stored, under the customer's control, in a safety deposit box"—not a bank's records. H.R. Rep. 99-647, at 23 n.41 (1986).[3]

[3] One of Congress's overarching goals was thus to protect private emails. Contrary to the Government's assertion (at 8), that intention is not belied by Congress's treatment of email content held for over 180 days, and email content sent to a "remote computing service" for long-term storage and processing. Congress considered those emails subject to the lesser protection of a subpoena, *see* § 2703(a), (b)(1)(B)(i), (b)(2), only because no one considered that content to be private, given the way email worked in 1986. At that time, private email rarely remained on a server for long. When a customer checked her email, it was downloaded to her personal computer and deleted from a server. Content left behind or shared with a provider for processing was considered a copy given to the provider for its use, and thus more like a business record, akin to documents disclosed to an accountant for processing. *See* Orin S. Kerr, *A User's Guide to the* (continued…)

The upshot is that when the Government seeks a customer's personal email content from a provider's servers, it must initiate a search and seizure. *That* is why Congress required and used the term "warrant," instead of creating a new hybrid "probable-cause subpoena." The Government may execute the search and seizure itself, by breaking down doors to retrieve the relevant servers, or (as is more common) it "may require the disclosure by a provider" conscripted to seize the content from its own servers on the Government's behalf. § 2703(a). This mirrors the physical world, where the Government can execute a search of a safe deposit box by using its own brute force, or by conscripting a bank's manager to open the designated box. Either way, it is a search and seizure that interferes with a customer's reasonable expectation of privacy in his personal belongings. OB 16 n.10, 25-26. A search is a search, whether conducted by a uniformed agent or "effected by a private individual . . . acting as an agent of the Government or with the participation or knowledge of any governmental official." *Jacobsen*, 466 U.S. at 113; s*ee also Gambino v. United States*, 275 U.S. 310, 316-17 (1927). Nor does it become any less of a search simply because the statute says the provider must "disclose" the emails to the Government after conducting the compelled search and seizure. "The issue is the nature of the governmental power being exercised, not the way it is labeled." U.S. Br. 10.

B. Execution Of This Search And Seizure Warrant Would Require Unauthorized Extraterritorial Application Of § 2703(a).

The Government's misstatement of what the Warrant commands Microsoft to do infects

---

Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1234 (2004); *see also* H.R. Rep. 99-647, at 68. The practices and expectations are the opposite now that cheap and plentiful storage allows us to retain a lifetime of private communications on secure remote servers. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 391-92 (2014). This fundamental change led the Sixth Circuit to invalidate these anachronistic provisions "to the extent that [they] purport[] to permit the government to obtain" *any* email content "warrantlessly." *Warshak*, 631 F.3d at 288.

its entire analysis of the central issue in this case—extraterritoriality. The Government asserts this case involves no unauthorized extraterritorial application of law because (1) "Microsoft is simply required to collect and produce its own records" to law enforcement officials, "similar to any subpoena recipient," and (2) under the *BNS* doctrine, any "need to retrieve records from abroad in order to" comply with such an order has only "incidental effects outside the country." U.S. Br. 14, 19. But since § 2703(a) requires a provider to do much more than produce its own business records, the *BNS* doctrine does not answer the extraterritoriality question. No case has ever extended the *BNS* doctrine to warrants authorizing the search and seizure of private effects safeguarded by a third party. Instead, the Court's analysis must begin with *Morrison*, and ask (1) whether the search occurs abroad; and (2) if so, whether § 2703(a) overcomes the presumption against extraterritorial application of statutes.

1. The search of emails residing on a Dublin server occurs abroad.

The Government does not dispute that the location of a search and seizure of electronic data is determined by the physical location of the data. OB 16 & n.10. Nor would it, because the Government wants to preserve its power to search and seize data residing on foreign servers without a warrant—which it can do if (and only if) the search occurs where the data, rather than the agent, is. The Government made—and prevailed on—this very argument in *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001), in which the court held that the Government's search had taken place overseas even though the FBI agents conducting the search were located in the U.S. And *Riley* has since explained, "Cloud computing is the capacity of Internet-connected devices to display data *stored on remote servers* rather than on the device itself." 134 S. Ct. at 2491 (emphasis added). Accordingly, a search of cloud data incident to an arrest could not be justified on the ground that the search was of a phone on the arrestee's person. *Id.* Similarly, whether Microsoft accesses a customer's email content

from a smart phone on the street or a terminal at its U.S. headquarters, the search occurs on the server where the data resides—here, in Dublin.

Rather than dispute this basic proposition, the Government insists (at 15 n.8) that there is no search or seizure when the provider finds the relevant emails, copies them, transmits them to the United States, and hands them over to law enforcement here—but only when agents open the file and read it. The Supreme Court has rejected that type of fiction. The search and seizure is effected by those who act at the government's behest "solely for the purpose of aiding the United States." *Gambino*, 275 U.S. at 316-17 (Brandeis, J.). Here, whether the intrusion into the account-owner's privacy is performed by an FBI agent sitting at Microsoft's U.S. headquarters or by a Microsoft technician acting as the Government's agent, and no matter where the data is reviewed, it is a search and seizure. And in this case, it occurs in Ireland.

The extraterritorial nature of this search and seizure would be even more clear had this Warrant met the Fourth Amendment's particularity requirement by naming the Dublin facility as the place to be searched, rather than describing in general terms Microsoft's 100 datacenters worldwide. *See* OB 26-27. The Government's cases (at 28-29) suggesting an electronic address suffices involve "live" surveillance with telephone wiretaps and mobile tracking devices, rather than communications in storage in a particular location, and thus are readily distinguishable. So too are the data-search cases cited by the Government (at 29), none of which considered a provider's challenge to a warrant on the ground that it authorized the Government to search all of the provider's datacenters worldwide. Instead, by suggesting that this is not a real "warrant" that must describe the place to be searched with particularity, the Government seeks to obfuscate the broad extraterritorial reach it would give ECPA.

2. Nothing in § 2703(a) overcomes the presumption against extraterritoriality.

The next question under *Morrison* is whether "'there is the affirmative intention of the Congress clearly expressed' to give a statute extraterritorial effect"; if there is not, courts "must presume [Congress] is primarily concerned with domestic conditions." 561 U.S. at 255 (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991) ("*Aramco*")). Likewise, *Charming Betsy* requires a clear statement before a statute may be read to violate international law norms. *See* OB 19-21. The Government points to no such "clear statement from Congress." *Bond v. United States*, 134 S. Ct. 2077, 2088 (2014). All the Government can muster is that "[n]othing in the text or structure of the statute carves out an exception for records stored abroad," and "nothing in the legislative history of [ECPA] indicates that Congress intended to artificially impose 'territorial' limits on warrants issued under the statute." U.S. Br. 2, 9. But that turns the presumption on its head: Congress must affirmatively indicate extraterritorial application, not "territorial limits." Silence means domestic application only. *See Bond*, 134 S. Ct. at 2088.

Congress did not affirmatively intend extraterritorial application. First, Congress in 1986 did not focus on the possibility of storing email on remote servers overseas. (Microsoft did not begin using foreign-based servers until 2010. A.B. Decl. ¶ 5.) Second, the Government does not even respond to our observation (at 20 n.12) that, had Congress contemplated extraterritorial warrants, it would not have authorized "State court[s]" to issue those warrants, § 2703(a), at the request of "a department or agency of . . . any State or political subdivision thereof," § 2711(4).[4] As the Supreme Court has held, only "the U.S. Government" reliably exercises the proper "de-

[4] State and local prosecutors use this warrant power regularly. *See, e.g., State v. Rose*, No. 10P3394, ___ P.3d ____, 2014 WL 2978315, at *3-*4 (Ct. App. Or. July 2, 2014); *Preventive Med. Assocs. v. Commonwealth*, 992 N.E.2d 257, 261 (Mass. 2013); *State v. Esarey*, 67 A.3d 1001, 1007 (Conn. 2013).

gree of self-restraint and consideration of foreign governmental sensibilities" in infringing sovereigns' interests. *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 171 (2004) (internal quotation marks omitted).

Third, as we have explained (at 18), the legislative history suggests that warrants issued pursuant to ECPA *are* limited to U.S. territory. Until 2001, § 2703(a) required "a warrant issued under the Federal Rules of Criminal Procedure." The Government does not dispute that the relevant Rule authorized only domestic warrants, with three narrow exceptions not relevant here. *See* Fed. R. Crim. P. 41(b). Congress then replaced "under the Federal Rules of Criminal Procedure" with "using the procedures described in the Federal Rules of Criminal Procedure," in order to create an exception to Rule 41(b) by allowing "*Nationwide* Service of Search Warrants for Electronic Evidence" outside of magistrate judges' home districts. Pub. L. No. 107-56, § 220(a)(1), 115 Stat. 291 (2001) (emphasis added); OB 18. But no Member of Congress or committee said a word about transforming § 2703(a) into a statute of worldwide application. It is inconceivable Congress would have taken so significant a step without discussion.

Nor does ECPA's definition of a "court of competent jurisdiction," § 2711(3), overcome the presumption. *Cf.* U.S. Br. 5-6. That provision says nothing about extraterritorial application. If anything, it suggests the opposite. Congress added the current language in 2009 to resolve an ambiguity that hindered the Government's handling of MLAT requests from foreign governments. *See* Foreign Evidence Request Efficiency Act, Pub. L. 111-79, 123 Stat. 2086 (2009).[5] Not only does this amendment lack any express indication of congressional intent to extend

[5] *See also* 155 Cong. Rec. S6810 (daily ed. June 18, 2009) (letter of the U.S. Department of Justice explaining the amendment's limited purpose and that "the proposed legislation would not in any way change the existing standards that the government must meet in order to obtain evidence, nor would it alter any existing safeguards on the proper exercise of such authority").

§ 2703(a) to email content stored abroad, but it demonstrates Congress's understanding that bilateral cooperation is the preferred mechanism for seizing email content from another country.

Because § 2703(a) "gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255. A warrant directing a provider to seize an account owner's email content from outside the United States is therefore invalid and unenforceable.

C. The Implications For International Comity Are Far More Grave Than With Standard Business Records Requests.

The presumption against extraterritoriality "applies regardless of whether there is a risk of conflict between the American statute and a foreign law." *Morrison*, 561 U.S. at 255. But because the risk here is grave—indeed, it has materialized—the Court must apply the presumption with special care. *See Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (citing "international discord" that "could result" from "unintended clashes between our laws and those of other nations"). We have described (OB 29-30 & n.19) the hostile reactions the Magistrate Judge's order immediately precipitated. And the international discord over this case grows each day. On June 24, the European Commissioner for Justice expressed "[t]he Commission's concern . . . that the extraterritorial application of foreign law (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the [EU]," while leaving "companies bound by EU data protection law . . . caught in the middle of . . . a conflict of laws." Catalano Supp. Decl., Ex. 1, at 2. Headlines across the world have protested, "US Wants To Rule Over All Servers Globally." Catalano Supp. Decl., Ex. 2. And the recent controversy over U.S. providers' compliance with the Government's demands for data has subjected those providers to investigations in foreign countries for violating their data privacy laws. Just last month, for example, the Irish High Court referred a case involving Facebook to the European Court of Justice. *See, e.g.*, Catalano Supp. Decl.,

Exs. 13, 14. There is nothing "rhetorical," U.S. Br. 17, or "speculative" about the fear that "unless [the U.S.] is required to use MLATs to obtain data stored abroad, U.S. foreign relations will be damaged and other countries will retaliate by asserting jurisdiction over electronic data stored here," U.S. Br. 26. The United Kingdom did it *last week*. Catalano Supp. Decl., Ex. 15, § 4.

The Government's only substantive response is *BNS*—again. *See* U.S. Br. 21 (citing Restatement § 442). The response is unavailing, for the same reason: Searches and seizures seeking "disclosure" of a customer's private property bear no resemblance to requests for production of a company's own records. Any country would view the invasion of a customer's privacy to seize his email content as a deployment of law-enforcement power, which may be "exercise[d] . . . in the territory of another state only with the consent of the other state." Restatement § 432(2). Our Government will too the moment the shoe is on the other foot: If a foreign government, with no notice to or collaboration with U.S. authorities, ordered Microsoft's employees in a local facility to connect to Microsoft's U.S. network and download all the content of a customer's email account stored in the U.S., our Government would express outrage. We would not brook the argument that the foreign state was asking Microsoft only to "disclose" its own business records or that the impact on U.S. territory is merely "incidental." U.S. Br. 19.[6] And seizing sensitive communications in violation of local law is even more of an affront to sovereign interests when it sidesteps established avenues for international cooperation. *See* OB 20-21.[7]

---

[6] Moreover, providers would be caught between their duties under foreign law to obey such demands and their obligation not to disclose email content under ECPA, which provides no exception for requests of *foreign* governments. *See* § 2702(b).

[7] Although the Ireland-U.S. MLAT contains no "exclusive use" requirement (*see* U.S. Br. 22 & n.13), it contemplates that other methods used will be through bilateral cooperation, *see* art. 17. The Government's approach here would hardly be considered performance of its treaty obligations "in good faith." *See* OB 20. Moreover, the assertion of unilateral authority at the expense of available avenues for cooperation causes discord as well, as foreign leaders' responses to this (continued…)

D. The Government Should Address Any Policy Concerns To Congress.

The Government worries its "ability to obtain [account owners' email content] from a provider would turn entirely on whether it happens to be stored here or abroad." U.S. Br. 23. But that possibility is nothing new. The Government needs bilateral cooperation to obtain a stack of correspondence sitting in a foreign safe deposit box or in a UPS envelope sitting in Dublin. Emails stored on a Dublin server are no different.[8] If Congress wants to grant the Federal Government and state and local officers the extraordinary power to unilaterally conscript providers to search and seize foreign email content—without even providing notice to the foreign country where the search and seizure is taking place—it may attempt to do so through a clear grant of that power. Until then, the Government cannot claim that power simply because it finds it more convenient. That international sovereignty may constrain U.S. law enforcement is no reason to disregard ECPA's text or the presumption against extraterritoriality.

In any event, bilateral methods work just as well for communications stored electronically as for any other physical documents or evidence. The Government can readily obtain emails stored in Ireland by making a request under the Ireland-U.S. MLAT, which, according to the former Minister of Justice and Attorney General of Ireland, was intended "to serve as *the means* for law enforcement authorities in the respective countries to obtain evidence located in the other treaty party." McDowell Decl. ¶ 2 (emphasis added). The Government has no response to Min-

---

litigation demonstrate. And that tension informs the interpretation of whether Congress intended to authorize such unilateral action abroad without saying so. *See Aramco*, 499 U.S. at 248. The ultimate question is not whether international law has been violated, but what power Congress intended to confer in § 2703(a).

[8] The Government argues (at 25) that unscrupulous providers may "choose to store user data abroad with the specific intent to place it out of the Government's reach." But if a criminal wants to place his emails out of the reach of U.S. authorities, all he has to do is open his account with a foreign provider, such as the Russian website, mail.ru.

ister McDowell's testimony that Ireland's MLAT procedures are "efficient and well-functioning," *id.* ¶ 8; nor does it address the State Department's representation to Congress that "[o]n mutual assistance requests, Irish police cooperate extensively with U.S. law enforcement agents." *Law Enforcement Treaties: Hearing Before the Committee on Foreign Relations of the United States Senate* (S. Hrg. 107-721), 107th Cong. 19 (2002).[9] Minister McDowell confirms that the Government's unsupported assertion about MLAT processing times is incorrect with respect to Ireland. McDowell Supp. Decl. ¶¶ 3-5. Indeed, the Government can seek to preserve the requested data at any time, day or night, and when a matter is urgent the two countries "move with great alacrity and efficiency in processing, transmitting, and responding to" MLAT requests. DeMarco Decl. ¶¶ 11-14.

In short, if the power ECPA grants the Government has failed to keep pace with its needs in a changing world, the Government is well-positioned to adapt appropriately, or to request that Congress make any necessary legislative amendments. But the Government may not arrogate to itself Congress's prerogative to decide whether, and under what circumstances, providers should be compelled execute searches and seizures of individuals' private content abroad.

III. Conclusion

For the foregoing reasons, this Court should vacate the warrant.

Dated: July 24, 2014

Respectfully submitted,

[9] The Government cites (at 26) two cases discussing MLAT delays, but neither involved Ireland. Even if the MLAT process involved delay, other mechanisms help ensure that evidence is preserved in the interim: The Government may immediately request the preservation of stored data under the Convention on Cybercrime, Council of Eur., Nov. 23, 2001, E.T.S. No. 185, art. 16-17. *See also* DeMarco Decl. (former head of the S.D.N.Y. U.S. Attorney's Office's Computer Hacking and Intellectual Property program) ¶¶ 3, 10-14 (describing the "several methods of evidence preservation that are used by the DOJ for the purpose of quickly, effectively, and efficiently ensuring that electronic communications and other digital evidence located abroad are preserved pending the execution of formal legal process to obtain such evidence").

/s/ Guy Petrilllo
Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkbllp.com
nboxer@pkbllp.com

/s/ E. Joshua Rosenkranz
E. Joshua Rosenkranz
Robert M. Loeb**
Brian P. Goldman**
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019-6142
Tel: 212.506.5380
jrosenkranz@orrick.com
rloeb@orrick.com
brian.goldman@orrick.com

Bradford L. Smith
David Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION

/s/ Nancy Kestenbaum
Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
nkestenbaum@cov.com
ccatalano@cov.com

James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
Fax: 202.662.6291
jgarland@cov.com
aberengaut@cov.com

**Admitted pro hac vice*
***Applications for admission pro hac vice pending*

Counsel for Microsoft Corporation